

0/520717

PCT/JPC3/08631

日 本 国 特 許 庁
JAPAN PATENT OFFICE

07.07.03

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2002年 7月10日

出 願 番 号
Application Number: 特願2002-201444
[ST. 10/C]: [JP2002-201444]

出 願 人
Applicant(s): シャープ株式会社

REC'D 22 AUG 2003

WIPO PCT

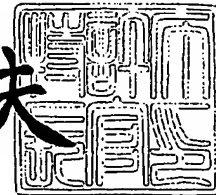
PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

CERTIFIED COPY OF
PRIORITY DOCUMENT

2003年 8月 7日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



出証番号 出証特2003-3063321

【書類名】 特許願

【整理番号】 02J01320

【提出日】 平成14年 7月10日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 9/32

【発明者】

 【住所又は居所】 大阪府大阪市阿倍野区長池町 2 2 番 2 2 号 シャープ株式会社内

 【氏名】 吉村 秀義

【特許出願人】

 【識別番号】 000005049

 【氏名又は名称】 シャープ株式会社

【代理人】

 【識別番号】 100075502

 【弁理士】

 【氏名又は名称】 倉内 義朗

 【電話番号】 06-6364-8128

【手数料の表示】

 【予納台帳番号】 009092

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 リライタブルメディアの改竄防止署名方法、この方法を実行する改竄防止署名装置、この装置を備えた改竄防止署名システム、この方法を実現するための改竄防止署名プログラムおよびこの改竄防止署名プログラムを記録したコンピュータ読み取り可能な記録媒体

【特許請求の範囲】

【請求項 1】 書き込みおよび消去可能な状態で記憶されている表示データを表示するリライタブルメディアに表示された表示データを認証するリライタブルメディアの改竄防止署名方法であって、

表示データを認証した認証者の指示により、表示データを読み込んで生成した画像データから特徴量を抽出する抽出工程と、

識別子と対になった暗号鍵を用いて、前記特徴量を暗号化することにより暗号化データを生成するデータ生成工程と、

これらの識別子と暗号化データとをリライタブルメディアに付加しておく付加工程と、

認証を確認する確認者の指示により、識別子を基に暗号鍵を取得し、暗号化データを復号した特徴量と表示データの特徴量とが一致するか否かを判定する判定工程と

からなることを特徴とするリライタブルメディアの改竄防止署名方法。

【請求項 2】 前記抽出工程において、表示データを読み込んで生成した画像データから抽出された大まかな特徴を特徴量として採用する請求項 1 記載のリライタブルメディアの改竄防止署名方法。

【請求項 3】 書き込みおよび消去可能な状態で記憶されている表示データを表示するリライタブルメディアに表示された表示データを認証するリライタブルメディアの改竄防止署名方法を実行する改竄防止署名装置であって、

表示データを認証した認証者の指示により、表示データを読み込んで生成した画像データの特徴を表す特徴量を抽出する特徴量抽出手段と、

識別子と対になった暗号鍵を用いて、前記特徴量を暗号化することにより暗号化データを生成するとともに、暗号化データを特徴量に復号化する暗号化・復号

化手段と、

識別子と暗号化データとをリライタブルメディアに付加する付加手段と、

復号化された特徴量と表示データの特徴量とが一致するか否かを判定する改竄判定手段と

を備えたことを特徴とする改竄防止署名装置。

【請求項 4】 書き込みおよび消去可能な状態で記憶されている表示データを表示するリライタブルメディアに表示された表示データを認証する改竄防止署名システムであって、

識別子の登録とともに、暗号鍵を生成する暗号鍵生成手段と、

識別子と暗号鍵とを保管する保管手段と、

識別子による問い合わせにより、暗号鍵を供給する認証手段と、

表示データを認証した認証者の指示により、表示データを読み込んで生成した画像データの特徴を表す特徴量を抽出する特徴量抽出手段と、識別子と対になった暗号鍵を用いて、前記特徴量を暗号化することにより暗号化データを生成するとともに、暗号化データを特徴量に復号化する暗号化・復号化手段と、識別子と暗号化データとをリライタブルメディアに付加する付加手段と、復号化された特徴量と表示データの特徴量とが一致するか否かを判定する改竄判定手段とを備え
てなる改竄防止署名装置と

からなることを特徴とする改竄防止署名システム。

【請求項 5】 書き込みおよび消去可能な状態で記憶されている表示データを表示するリライタブルメディアに表示された表示データを認証するリライタブルメディアの改竄防止署名方法を実現するための改竄防止署名プログラムであって、

表示データを認証した認証者の指示により、表示データを読み込んで生成した画像データから特徴量を抽出する抽出工程と、

識別子と対になった暗号鍵を用いて、前記特徴量を暗号化することにより暗号化データを生成するデータ生成工程と、

これらの識別子と暗号化データとをリライタブルメディアに付加しておく付加工程と、

認証を確認する確認者の指示により、識別子を基に暗号鍵を取得し、暗号化データを復号した特徴量と表示データの特徴量とが一致するか否かを判定する判定工程と

からなることを特徴とする改竄防止署名方法を実現するための改竄防止署名プログラム。

【請求項 6】 請求項 5 記載の改竄防止署名プログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、表示データの書き込みおよび消去ができるリライタブルメディアの改竄防止署名方法、この方法を実行する改竄防止署名装置、この装置を備えた改竄防止署名システム、この方法を実現するための改竄防止署名プログラムおよびこの改竄防止署名プログラムを記録したコンピュータ読み取り可能な記録媒体に関するものである。特に、表示データの改竄の防止を行うためのリライタブルメディアの改竄防止署名方法、この方法を実行する改竄防止署名装置、この装置を備えた改竄防止署名システム、この方法を実現するための改竄防止署名プログラムおよびこの改竄防止署名プログラムを記録したコンピュータ読み取り可能な記録媒体に関するものである。

【0002】

【従来の技術】

従来、契約書等といった紙を用いた証明物を扱うときには、証明者がボールペンで署名を行ったり、インクを用いて捺印等を行ったりすることにより、内容を確認したことの証明を行っていた。しかし、このような紙を用いた証明物においては、不要になった場合に、インク等が紙中に浸透しているために文字などを消して紙を再利用することができないといった問題があった。

【0003】

そこで、近年、資源の有効利用の観点から、紙を用いない証明物の利用が注目されている。紙を用いることなく証明物を作成する際に利用される改竄防止署名

システムおよびこのシステムを用いて実施される改竄防止署名方法の一従来例として、例えば、特開平11-261550号公報に開示されている電子文書の改竄防止システムおよび方法がある。この電子文書の改竄防止システムおよび方法において用いられている電子署名技術署名では、電子データから抽出した特徴量を、秘密鍵を用いて暗号化して電子データに添付して送付するといったものである。そして、電子データ受領者は公開鍵を暗号化された特徴量を用いて復号化し、受け取った電子データの特徴量と復号化した特徴量との一致を確かめることで、受け取った電子データが改竄されていないことを確認している。

【0004】

また、紙を用いない証明物の一従来例として、特開2000-313185号公報に開示されているリライト表示部を有した非接触IC（集積回路）証明書がある。この非接触IC証明書はリライタブルメディアのリライト表示部に表示されるものであり、リライタブルメディアとは、電氣的、磁氣的、または熱的といったような外的要因によって、表示データの内容の書き込みおよび消去を行う装置であり、例えば、トナーを含有したマイクロカプセルを用いたデバイス、強誘電液晶を用いたデバイス、およびロイコ染料を用いたデバイス等があり、このリライタブルメディアを用いて作成された証明物は再利用が可能である。

【0005】

【発明が解決しようとする課題】

しかしながら、前述した電子署名技術においては、証明物が電子文書であることが前提となり、証明を行う際には必ず閲覧用装置が必要であるため、メディア単体で証明が行えないといった問題があった。

【0006】

一方、前述した非接触IC証明書を表示するリライタブルメディアにおいては、リライタブルメディア自体が記録された表示データを証明するといった機能を備えたものではないため、証明書発行に煩雑な過程が必要であるといった問題があった。

【0007】

本発明はこのような問題を解決すべく創案されたものであり、メディア単体で

簡単に証明を行うことができるリライタブルメディアの改竄防止署名方法、この方法を実行する改竄防止署名装置、この装置を備えた改竄防止署名システム、この方法を実現するための改竄防止署名プログラムおよびこの改竄防止署名プログラムを記録したコンピュータ読み取り可能な記録媒体を提供することを目的とする。

【0008】

【課題を解決するための手段】

本発明のリライタブルメディアの改竄防止署名方法は、書き込みおよび消去可能な状態で記憶されている表示データを表示するリライタブルメディアに表示された表示データを認証するリライタブルメディアの改竄防止署名方法であって、表示データを認証した認証者の指示により、表示データを読み込んで生成した画像データから特徴量を抽出する抽出工程と、識別子と対になった暗号鍵を用いて、前記特徴量を暗号化することにより暗号化データを生成するデータ生成工程と、これらの識別子と暗号化データとをリライタブルメディアに付加しておく付加工程と、認証を確認する確認者の指示により、識別子を基に暗号鍵を取得し、暗号化データを復号した特徴量と表示データの特徴量とが一致するか否かを判定する判定工程とからなるものである。

【0009】

この発明によれば、書き込みおよび消去可能な状態で記憶されている表示データを表示するリライタブルメディアの表示データの内容を認証したときに、認証者の指示により、表示データを読み込んで特徴量をデータ化し、暗号化して、リライタブルメディアに付加することができる。このとき、認証者の署名データ等の図形データである識別子もリライタブルメディアに付加される。さらに、暗号化・復号化の暗号鍵はこの識別子と対になって生成されており、リライタブルメディアを受け取った側はこの識別子により暗号鍵を取得し、復号化ができる。その結果、認証時の表示データの特徴量を取得して、この特徴量と現在表示されている表示データの特徴量とを比較して、一致するか否かを判定することができる。

【0010】

なお、リライタブルメディアとは、電氣的、磁氣的または熱的に書き込みおよび消去が可能なメディアであり、具体的には、液晶を用いたメディア、ロイコ染料を用いたメディアおよびカプセルトナーを用いたメディア等が挙げられる。

【0011】

また、本明細書において、特徴量とは、表示データの読み込みデータの特徴を表したものである。例えば、エッジを明確にした表示文字の形状から計算した値や、表示内容を電氣的に読み出せるリライタブルメディアにおいては、表示内容そのものから計算して特徴量を得てもよい。

【0012】

さらにまた、暗号化データの記録方法としては、バーコードや、磁性層を設けることで磁氣的に記録してもよく、また、ICチップを搭載して記録してもよい。

【0013】

また、前記抽出工程において、表示データを読み込んで生成した画像データから抽出された大まかな特徴を特徴量として採用してもよい。

【0014】

この場合には、照合時に、画像データの読み取り時の揺らぎ等で、現在表示している画像データが暗号化データの画像データと画素単位で完全に一致しない場合でも、特徴量は同一となり一致とみなされ、改竄なしと判断することができる。

【0015】

ここでは、大まかな特徴とは、画像を折れ線近似した場合の各要素の重心、傾きおよび線の長さ等を示す。

【0016】

本発明の改竄防止署名装置は、書き込みおよび消去可能な状態で記憶されている表示データを表示するリライタブルメディアに表示された表示データを認証するリライタブルメディアの改竄防止署名方法を実行する改竄防止署名装置であって、表示データを認証した認証者の指示により、表示データを読み込んで生成した画像データの特徴を表す特徴量を抽出する特徴量抽出手段と、識別子と対にな

った暗号鍵を用いて、前記特徴量を暗号化することにより暗号化データを生成するとともに、暗号化データを特徴量に復号化する暗号化・復号化手段と、識別子と暗号化データとをリライタブルメディアに付加する付加手段と、復号化された特徴量と表示データの特徴量とが一致するか否かを判定する改竄判定手段とを備えたものである。

【0017】

この発明によれば、書き込みおよび消去可能な状態で記憶されている表示データを表示するリライタブルメディアの表示データの内容を認証したときに、認証者の指示により、表示データを読み込んで特徴量をデータ化し、暗号化して、リライタブルメディアに付加することができる。このとき、認証者の署名データ等の図形データである識別子もリライタブルメディアに付加される。さらに、暗号化・復号化の暗号鍵はこの識別子と対になって生成されており、リライタブルメディアを受け取った側はこの識別子により暗号鍵を取得し、復号化ができる。その結果、認証時の表示データの特徴量を取得して、この特徴量と現在表示されている表示データの特徴量とを比較して、一致するか否かを判定することができる。

【0018】

本発明の改竄防止署名システムは、書き込みおよび消去可能な状態で記憶されている表示データを表示するリライタブルメディアに表示された表示データを認証する改竄防止署名システムであって、識別子の登録とともに、暗号鍵を生成する暗号鍵生成手段と、識別子と暗号鍵とを保管する保管手段と、識別子による問い合わせにより、暗号鍵を供給する認証手段と、表示データを認証した認証者の指示により、表示データを読み込んで生成した画像データの特徴を表す特徴量を抽出する特徴量抽出手段と、識別子と対になった暗号鍵を用いて、前記特徴量を暗号化することにより暗号化データを生成するとともに、暗号化データを特徴量に復号化する暗号化・復号化手段と、識別子と暗号化データとをリライタブルメディアに付加する付加手段と、復号化された特徴量と表示データの特徴量とが一致するか否かを判定する改竄判定手段とを備えてなる改竄防止署名装置とからなるといったものである。

【0019】

この発明によれば、書き込みおよび消去可能な状態で記憶されている表示データを表示するリライタブルメディアの表示データの内容を認証したときに、認証者の指示により、表示データを読み込んで特徴量をデータ化し、暗号化して、リライタブルメディアに付加することができる。このとき、認証者の署名データ等の図形データである識別子もリライタブルメディアに付加される。さらに、暗号化・復号化の暗号鍵はこの識別子と対になって生成されており、リライタブルメディアを受け取った側はこの識別子により暗号鍵を取得し、復号化ができる。その結果、認証時の表示データの特徴量を取得して、この特徴量と現在表示されている表示データの特徴量とを比較して、一致するか否かを判定することができる。

【0020】

本発明の改竄防止署名プログラムは、書き込みおよび消去可能な状態で記憶されている表示データを表示するリライタブルメディアに表示された表示データを認証するリライタブルメディアの改竄防止署名方法を実現するための改竄防止署名プログラムであって、表示データを認証した認証者の指示により、表示データを読み込んで生成した画像データから特徴量を抽出する抽出工程と、識別子と対になった暗号鍵を用いて、前記特徴量を暗号化することにより暗号化データを生成するデータ生成工程と、これらの識別子と暗号化データとをリライタブルメディアに付加しておく付加工程と、認証を確認する確認者の指示により、識別子を基に暗号鍵を取得し、暗号化データを復号した特徴量と表示データの特徴量とが一致するか否かを判定する判定工程とからなる改竄防止署名方法を実現するものである。

【0021】

この発明によれば、書き込みおよび消去可能な状態で記憶されている表示データを表示するリライタブルメディアの表示データの内容を認証したときに、認証者の指示により、表示データを読み込んで特徴量をデータ化し、暗号化して、リライタブルメディアに付加することができる。このとき、認証者の署名データ等の図形データである識別子もリライタブルメディアに付加される。さらに、暗号

化・復号化の暗号鍵はこの識別子と対になって生成されており、リライタブルメディアを受け取った側はこの識別子により暗号鍵を取得し、復号化ができる。その結果、認証時の表示データの特徴量を取得して、この特徴量と現在表示されている表示データの特徴量とを比較して、一致するか否かを判定することができる。

【0022】

本発明の改竄防止署名プログラムを記録したコンピュータ読み取り可能な記録媒体は、書き込みおよび消去可能な状態で記憶されている表示データを表示するリライタブルメディアに表示された表示データを認証するリライタブルメディアの改竄防止署名方法を実現するための改竄防止署名プログラムであって、表示データを認証した認証者の指示により、表示データを読み込んで生成した画像データから特徴量を抽出する抽出工程と、識別子と対になった暗号鍵を用いて、前記特徴量を暗号化することにより暗号化データを生成するデータ生成工程と、これらの識別子と暗号化データとをリライタブルメディアに付加しておく付加工程と、認証を確認する確認者の指示により、識別子を基に暗号鍵を取得し、暗号化データを復号した特徴量と表示データの特徴量とが一致するか否かを判定する判定工程とからなる改竄防止署名方法を実現する改竄防止署名プログラムを記録したものである。

【0023】

この発明によれば、書き込みおよび消去可能な状態で記憶されている表示データを表示するリライタブルメディアの表示データの内容を認証したときに、認証者の指示により、表示データを読み込んで特徴量をデータ化し、暗号化して、リライタブルメディアに付加することができる。このとき、認証者の署名データ等の図形データである識別子もリライタブルメディアに付加される。さらに、暗号化・復号化の暗号鍵はこの識別子と対になって生成されており、リライタブルメディアを受け取った側はこの識別子により暗号鍵を取得し、復号化ができる。その結果、認証時の表示データの特徴量を取得して、この特徴量と現在表示されている表示データの特徴量とを比較して、一致するか否かを判定することができる。

【0024】

【発明の実施の形態】

次に、本発明のリライタブルメディアの改竄防止署名方法、この方法を実行する改竄防止署名装置、この装置を備えた改竄防止署名システム、この方法を実現するための改竄防止署名プログラムおよびこの改竄防止署名プログラムを記録したコンピュータ読み取り可能な記録媒体の実施の形態について、図面を参照しつつ説明する。

【0025】

図1は、本発明の改竄防止署名システムの実施の形態1を示す説明図である。

【0026】

この改竄防止署名システムは、暗号鍵生成手段としての個人情報生成装置12と、保管手段としての個人情報保管装置13と、認証手段としての認証局14と、リライタブルメディア11と、改竄防止署名装置10a、10bとから構成されている。

【0027】

ここでは、認証者が、署名書き込み側である、図1の左側に図示されている個人情報生成装置12と個人情報保管装置13と改竄防止署名装置10aとを用いて、リライタブルメディア11に表示された表示データ1を認証して署名を行っており、さらに、認証者による署名後、確認者が、署名確認側である、図1の右側に図示されている認証局14と改竄防止署名装置10bとを用いて、リライタブルメディア11に表示される表示データ1が改竄されていないかを確認している。

【0028】

個人情報生成装置12は、ユーザが選択した任意の図形データを署名としてデータ化した署名データ（即ち、識別子）2を生成し、この署名データ2と対になっている、公開鍵暗号方式（例えば1977年にマサチューセッツ工科大学のリベスト（Rivest）、シャミア（Shamir）、エーデルマン（Adleman）の3人によって発案された公開鍵暗号方式であるRSA公開鍵暗号方式）による秘密鍵（即ち、暗号鍵）7および公開鍵（即ち、暗号鍵）5を生成する

ものである。

【0029】

また、個人情報保管装置 13 は、例えばフラッシュメモリカード等で構成されており、個人情報生成装置 12 によって生成した署名データ 2 と秘密鍵 7 とを保存しており、署名データ 2 と秘密鍵 7 とを署名書き込み側の改竄防止署名装置 10a に供給するものである。

【0030】

さらに、認証局 14 は、署名データ 2 とその対となっている公開鍵 5 とを保存しており、署名確認側が署名データ 2 を用いて問い合わせを行うことにより、改竄防止署名装置 10b に対象情報 6 と公開鍵 7 とを供給するものである。

【0031】

図 2 は、図 1 に示す改竄防止署名システムとともに使用されるリライタブルメディアの一例を示す説明図である。

【0032】

リライタブルメディア 11 は、情報記載域 109 と、複数の署名領域（ここでは、第 1 承認者の署名領域 105、第 2 承認者の署名領域 106、第 3 承認者の署名領域 107 および第 4 承認者の署名領域 108 がある）と、2 次元バーコード記載域（ここでは、第 1 承認者の暗号化データ 2 次元バーコード記載域 101、第 2 承認者の暗号化データ 2 次元バーコード記載域 102、第 3 承認者の暗号化データ 2 次元バーコード記載域 103 および第 4 承認者の暗号化データ 2 次元バーコード記載域 104 がある）とからなり、表示データ 1 および署名データ 2 を記録するものである。さらに、情報記載域 109 には、文書や、図形等の表示データ 1 が表示されている。また、第 1 承認者の署名領域 105、第 2 承認者の署名領域 106、第 3 承認者の署名領域 107 および第 4 承認者の署名領域 108 には、表示データ 1 を認証した認証者の署名データ 2 が記録されている。なお、認証者が複数いる場合は、複数の署名データ 2 が各署名領域に一つずつ記載される。さらにまた、第 1 承認者の暗号化データ 2 次元バーコード記載域 101、第 2 承認者の暗号化データ 2 次元バーコード記載域 102、第 3 承認者の暗号化データ 2 次元バーコード記載域 103 および第 4 承認者の暗号化データ 2 次元バ

ーコード記載域 104 には、認証時の表示データ 1 を暗号化した暗号化データ 3 がバーコードとして記録されている。なお、記録される位置は、署名された順番に対応して決められている。

【0033】

図 3 は、本発明の改竄防止署名装置の一実施の形態を示す説明図である。

【0034】

改竄防止署名装置 10a, 10b は、コンソール 36 と、改竄判定手段としてのコントローラ 37 と、メディア読み取り部 30 と、領域認識部 31 と、入力補正部 32 と、特徴量抽出手段としての特徴抽出部 33 と、付加手段としてのメディア書き込み部 34 と、暗号化・復号化手段としての暗号化・復号化部 35 と、認証局通信装置 38 と、個人情報保管装置 I/F (interface) 39 とから構成されており、署名データ 2 の書き込み、表示データ 1 の確認を行うものである。

【0035】

コンソール 36 は、ユーザが指示および選択を行う際や、ユーザにデータを示す際に使用されるものであり、キーボードやモニタ等といった装置を備えている。

【0036】

コントローラ 37 は、汎用の CPU (central processing unit) で構成されており、改竄判定手段として機能するのみならず改竄防止署名装置の一連の動作をコントロールするものである。

【0037】

メディア読み取り部 30 は、リライタブルメディア 11 の表示面全体を光学的に読み取り、読み取った情報を電気信号に変換するものである。図示しない CCD (charge coupled device) ラインイメージセンサユニットと副走査方向駆動系とを備えており、リライタブルメディア 11 を走査して、一主走査ライン毎に RGB (「R」は「赤」の略であり、「G」は「緑」の略であり、「B」は「青」の略である。) カラー信号を生成し、この RGB カラー信号を有効範囲のみ A/D (analog to Digital) 変換してデ

デジタルデータに変換し、領域認識部 31 に出力する。

【0038】

領域認識部 31 は、入力データに対して処理を行い、図 2 に示す署名領域、2 次元バーコード記載域およびその他の領域等といった各領域の判別を行い、領域判別後の入力画像データを入力補正部 32 に出力するものである。

【0039】

入力補正部 32 は、領域判別後の入力画像データを用いてスキュー補正および倍率補正を行い、入力データを補正し、補正後の入力データを特徴抽出部 33 に出力するものである。

【0040】

特徴抽出部 33 は、補正後の入力データに対して、領域認識部 31 が判別した領域認識結果に基づいて、署名領域と 2 次元バーコード記載域とを除いた領域に関して、入力画像データから特徴量を抽出し、抽出した特徴量を示すデータを暗号化・復号化装置 35 に出力するものである。

【0041】

暗号化・復号化装置 35 は、コントローラ 37 からの指示により、特徴量の暗号化または暗号化データの復号化を行うものである。

【0042】

メディア書き込み部 34 は、署名データ 2 および 2 次元バーコード記載域をリライタブルメディア 11 に書き込むものである。

【0043】

認証局通信装置 38 は、電話回線またはインターネット通信網等といったネットワーク回線を用いて認証局 14 との間で通信を行い、署名データ 2 を用いた問い合わせや公開鍵の取得等を行うものである。

【0044】

個人情報保管装置 I/F 39 は、個人情報保管装置 13 とのインタフェースを取りもつものであり、署名データ 2 や秘密鍵の取得等を行うものである。

【0045】

次いで、このような構成を備えた改竄防止署名システムを用いたリライタブル

メディアの改竄防止署名方法について説明する。

【0046】

図4～図6は、本発明のリライタブルメディアの改竄防止署名方法の一実施の形態を示すフローチャートであり、図4は、署名を書き込む手順を示すフローチャートであり、図5は、署名を確認する手順を示すフローチャートであり、図6は、特徴量を抽出する手順を示すフローチャートである。

【0047】

まず初めに、図4を参照しつつ、認証者が新たな表示データ1aを認証して、新たな署名データ2aをリライタブルメディアに書き込むフローを説明する。

【0048】

まず、既書き込まれている署名データ2があるか否かを確認し（ステップS1）、もし、署名データ2がある場合（ステップS1での判断結果がはいである場合）には、署名データ2が認証局に登録されているか否かを確認する（ステップS2）。

【0049】

もし、署名データ2が認証局に登録されている場合（ステップS2での判断結果がはいである場合）には、表示データ1が改竄されているか否かを確認する（ステップS3）。

【0050】

ここで、署名データ2が認証局に登録されていない場合（ステップS2での判断結果がいいえである場合）、または署名データ2が認証局に登録されているが表示データ1が改竄されていた場合（ステップS2およびステップS3での判断結果がはいである場合）には、新たな第1署名データ2の書き込みを中止し（ステップS4）、処理を終了する。

【0051】

一方、署名データ2がない場合（ステップS1での判断結果がいいえである場合）、または表示データ1が改竄されていない場合（ステップS3での判断結果がいいえである場合）には、リライタブルメディアの表示面全体を読み取り（ステップS5）、さらに、読み取った画像データに関して、2次元バーコード記載

域、署名領域および情報記載域それぞれを認識する（ステップS6）。

【0052】

次いで、入力画像がスキューをもっている場合、すなわち図8に示すように、リライタブルメディア11の水平線と読み取りにおける水平線との角度差がある場合には、そのスキュー角度50を情報記載域の周辺エッジ角度51から判別し、そのスキューをアフィン変換で補正する等といった画像補正を実行して表示データを得る（ステップS7）。

【0053】

そして、このような手順によって得られた表示データの特徴を抽出し（ステップS8）、さらに、特徴抽出によって得られた符号データ列からMD5（Message-Digest Algorithm 5 RFC1321）で16バイトのハッシュ値を取得することによって特徴量を計算する（ステップS9）。

【0054】

続いて、取得したハッシュ値を、個人情報保管装置から得た秘密鍵を用いて暗号化する（ステップS10）。

【0055】

最後に、既にかき込まれていた署名データ2の次の欄に、個人情報保管装置から読み出した新たな署名データ2aをかき込むとともに、暗号化したハッシュ値（新たな暗号化データ3a）を2次元バーコードに変換してかき込む（ステップS11）。

【0056】

次に、図5を参照しつつ、署名後の新たな表示データ1aに関して改竄の有無を確認する手順、即ち、新たな表示データ1aと現在表示されている表示データ1bとが同一の表示データであるか否かを確認するフローを説明する。

【0057】

まず、リライタブルメディアの表示面全体を読み取り（ステップS21）、さらに、読み取った画像データに関して、2次元バーコード記載域、署名領域および情報記載域それぞれを認識する（ステップS22）。

【0058】

次いで、入力画像がスキューをもっている場合には、そのスキュー角度を情報記載域の周辺エッジ角度から判別し、そのスキューをアフィン変換で補正する等といった画像補正を実行して表示データを得る（ステップS23）。

【0059】

このような手順を実行することによって、リライタブルメディアから、情報記載域に現在表示されている表示データ1bと署名データ2とを得る。

【0060】

続いて、既にかき込まれている全ての署名データ2の中で、確認が終了していないものがあるか否かを判断し（ステップS24）、もし、確認が終了していないものがある場合（ステップS24での判断結果がいいえである場合）には、ステップS25に進み、もし、確認が終了していないものがない場合（ステップS24での判断結果がはいである場合）には処理を終了する。

【0061】

ステップS25では、署名領域の最後に記載された署名データ2を認証局に送信して、照会を行う。例えば、第1署名領域から第3署名領域までに署名データが記載されているときには、第3署名領域に記載されている新たな署名データ2aを認証局に送信して、照会を行う。

【0062】

そして、例えば、新たな署名データ2aの読み取りを失敗していた等といった理由等によって、認証局にこの新たな署名データ2aが登録されていないと判断された場合（ステップS26での判断結果がいいえである場合）には、照会ができないので、その旨をユーザに警告通知して（ステップS27）、処理を終了する。

【0063】

一方、新たな署名データ2aが認証局に登録されていた場合（ステップS26での判断結果がはいである場合）には、認証局から新たな署名データ2aに対応する登録者情報4aと公開鍵5aとを受け取るとともに、リライタブルメディアから新たな署名データ2aに対応する2次元バーコード記載域から2次バーコードを読み取り、暗号化データ3aを得る（ステップS28）。

【0064】

続いて、暗号化データ 3 a を公開鍵 5 a を用いて復号化して、認証された表示データ 1 a の特徴量 A を得る（ステップ S 29）。そして、前述したステップ S 21 で読み取ったリライタブルメディアの情報記載域に表示されている表示データ 1 b から特徴量を抽出し（ステップ S 30）、特徴量 B を計算する（ステップ S 31）。

【0065】

その後、情報記載域に表示されている特徴量 B と認証された特徴量 A とを比較して（ステップ S 32）、情報記載域に表示されている特徴量 B と認証された特徴量 A とが一致しているか否かを判定する（ステップ S 33）。

【0066】

もし、一致している場合（ステップ S 33 での判断結果がはいである場合）には、処理の対象となっている署名データ 2 について、書き込み時からの改竄はないとみなし、ステップ S 24 に戻り、残りの署名データ 2 に関して、照会と特徴量の比較と（ステップ S 24 ～ステップ S 33）を署名データ 2 の数だけ繰り返し実行する。そして、全ての署名データ 2 に関して処理を終了したときには、ステップ S 24 で確認終了したと判断されるので（ステップ S 24 での判断結果がはいになるので）、処理を終了する。

【0067】

一方、ステップ S 33 において一致していないと判断された場合（ステップ S 33 での判断結果がいいえである場合）には、処理の対象となっている署名データ 2 について、書き込み後に改竄がなされたとみなし、コンソールを通じてユーザに対して警告通知を行い（ステップ S 27）、処理を終了する。

【0068】

次に、改竄防止署名装置を構成する特徴抽出部の動作について、図 6 を参照しつつ説明する。

【0069】

ここでは、リライタブルメディアの表示が電子的に読み出せない場合を例に挙げて説明する。

【0070】

表示データ1の読み込み時には、例えば図7(a)に示すような画像データ(太線の「A」)41が読み込まれるので、この画像データを用いてエッジ抽出する。このエッジ抽出では、まず、対象画素P1(x, y)の画素濃度を表す画素値p1(x, y)から、対象画像P1の左の画素P2の画素値p2(x-1, y)を減算し、減算によって得られた値の絶対値が閾値(Tedge)以上であれば、対象画素P1がエッジ画素であると判定する。そして、処理の対象となっている画像データを構成する全ての画素について、エッジ画素とそれ以外の画素とで2値化する。その後、画像データの左上から順に全ての画素について水平方向および垂直方向の順に走査し、検出したエッジ画素を基点として画像データ中のエッジ画素で囲まれた領域の輪郭線追跡を行う(ステップS41)。その結果、例えば、図7(b)に示すような輪郭線データ42を得る。

【0071】

続いて、輪郭線データを参照して、輪郭線で囲まれた領域について細線化処理を行い(ステップS42)、その結果、例えば、図7(c)に示すような細線43を得る。その後、得られた細線を直線化して折れ線近似し(ステップS43)、その結果、例えば、図7(d)に示すような近似画像44を得る。

【0072】

次いで、得られた近似画像を参照して、画像データの左上から全ての画素について順に水平方向および垂直方向の順に走査し、折れ線の重心点を発見した順に折れ線をナンバリングする。さらに、ナンバリングされた折れ線の順に、折れ線重心点(x_i, y_i)、折れ線長L_i、折れ線の水平からの角度θ_iのそれぞれのパラメータを抽出する(ステップS44)。

【0073】

最後に、抽出したパラメータをそれぞれ量子化し、さらに、量子化した各値をナンバリングの順に連結して符号データ列を作成する(ステップS45)。この際に、読み取り時の誤差を考慮して、読み取り時に判別が可能なパラメータのみを結合することが好ましい。

【0074】

また、前述した手順、即ち、リライタブルメディアの改竄防止署名方法は改竄防止署名プログラムによって実現される。さらに、改竄防止署名装置のコントローラ37には、この改竄防止署名プログラムを記録したコンピュータ読み取り可能な記録媒体が含まれている。この記録媒体としては、マスクROM (Read Only Memory) およびフラッシュROMといった半導体記憶素子、ハードディスク、フレキシブルディスク、MO (Magnetooptical Disk)、CD (Compact Disc) -ROM、DVD (Digital Versatile Disk) -ROM、光磁気ディスク、IC (Integrated Circuit) カード、および磁気テープ等をあげることができ、プログラムを記憶することが可能であれば、他の記録媒体であってもよい。また、プログラムそのものを通信により伝送して記録媒体に記録するといったものであってもよい。

【0075】

以上のように、本発明のリライタブルメディアの改竄防止署名方法、この方法を実行する改竄防止署名装置、この装置を備えた改竄防止署名システム、この方法を実現するための改竄防止署名プログラムおよびこの改竄防止署名プログラムを記録したコンピュータ読み取り可能な記録媒体によれば、表示データに暗号化された特徴量と、その識別子とが付加されるので、リライタブルメディア単体で、表示データに改竄があるかどうかを簡単に判別することができる。

【0076】

また、表示内容を大まかに抽出して、エッジが明確な文字の形状情報など、情報の本質から特徴量を抽出するので、例えば、リライタブルメディアの表示内容を複写機でコピーして得られた複写物においても、署名データの有効性を確認することができる。

【0077】

さらにまた、リライタブルメディアが表示内容読み出し機能を備えており、電子的に表示データを値として読み出すことが可能なメディアである場合、またはエラー訂正技術等によって、読み出しエラー率が十分に低いリライタブルメディアと改竄防止署名装置とを用いている場合においては、表示データの読み取りデ

ータ列を連結したものを符号データ列として用いてもよい。この場合には、前述した手順を実施すると、表示内容そのものから特徴量を抽出しているのので、表示データが署名時と完全に同じであることを確認することができる。

【0078】

一方、リライタブルメディア上での暗号化データの記録手段は、2次元バーコードに限定されず、磁性層を設けることで磁気的に記録してもよく、また、ICチップを搭載することで、ICチップに表示データを電子化したデータと暗号化データとを同時に記録するようにしてもよい。

【0079】

なお、リライタブルメディア上の各領域（署名領域、2次バーコード記載域および情報記載域）は位置を固定化しなくてもよい。このように、位置を固定化しない場合には、領域判別によって各領域に分離して処理を進めることができる。また、署名データに関しては、類推されるものをすべて認証局に問い合わせることで判別すればよい。

【0080】**【発明の効果】**

本発明のリライタブルメディアの改竄防止署名方法は、書き込みおよび消去可能な状態で記憶されている表示データを表示するリライタブルメディアに表示された表示データを認証するリライタブルメディアの改竄防止署名方法であって、表示データを認証した認証者の指示により、表示データを読み込んで生成した画像データから特徴量を抽出する抽出工程と、識別子と対になった暗号鍵を用いて、前記特徴量を暗号化することにより暗号化データを生成するデータ生成工程と、これらの識別子と暗号化データとをリライタブルメディアに付加しておく付加工程と、認証を確認する確認者の指示により、識別子を基に暗号鍵を取得し、暗号化データを復号した特徴量と表示データの特徴量とが一致するか否かを判定する判定工程とからなるといったものであり、この発明によれば、表示データとともに認証時の特徴量が付加されるので、リライタブルメディア単体で、表示データに認証後の改竄があるか否かを簡単に判別することができる。

【0081】

また、前記抽出工程において、表示データを読み込んで生成した画像データから抽出された大まかな特徴を特徴量として採用してもよく、この場合には、リライタブルメディアの表示部を複写機を用いてコピーした場合においても、認証を行うことができる。

【0082】

本発明の改竄防止署名装置は、書き込みおよび消去可能な状態で記憶されている表示データを表示するリライタブルメディアに表示された表示データを認証するリライタブルメディアの改竄防止署名方法を実行する改竄防止署名装置であって、表示データを認証した認証者の指示により、表示データを読み込んで生成した画像データの特徴を表す特徴量を抽出する特徴量抽出手段と、識別子と対になった暗号鍵を用いて、前記特徴量を暗号化することにより暗号化データを生成するとともに、暗号化データを特徴量に復号化する暗号化・復号化手段と、識別子と暗号化データとをリライタブルメディアに付加する付加手段と、復号化された特徴量と表示データの特徴量とが一致するか否かを判定する改竄判定手段とを備えたものであり、この発明によれば、表示データとともに認証時の特徴量が付加されるので、リライタブルメディア単体で、表示データに認証後の改竄があるか否かを簡単に判別することができる。

【0083】

本発明の改竄防止署名システムは、書き込みおよび消去可能な状態で記憶されている表示データを表示するリライタブルメディアに表示された表示データを認証する改竄防止署名システムであって、識別子の登録とともに、暗号鍵を生成する暗号鍵生成手段と、識別子と暗号鍵とを保管する保管手段と、識別子による問い合わせにより、暗号鍵を供給する認証手段と、表示データを認証した認証者の指示により、表示データを読み込んで生成した画像データの特徴を表す特徴量を抽出する特徴量抽出手段と、識別子と対になった暗号鍵を用いて、前記特徴量を暗号化することにより暗号化データを生成するとともに、暗号化データを特徴量に復号化する暗号化・復号化手段と、識別子と暗号化データとをリライタブルメディアに付加する付加手段と、復号化された特徴量と表示データの特徴量とが一致するか否かを判定する改竄判定手段とを備えてなる改竄防止署名装置とからな

るといったものであり、この発明によれば、表示データとともに認証時の特徴量が付加されるので、リライタブルメディア単体で、表示データに認証後の改竄があるか否かを簡単に判別することができる。

【0084】

本発明の改竄防止署名プログラムは、書き込みおよび消去可能な状態で記憶されている表示データを表示するリライタブルメディアに表示された表示データを認証するリライタブルメディアの改竄防止署名方法を実現するための改竄防止署名プログラムであって、表示データを認証した認証者の指示により、表示データを読み込んで生成した画像データから特徴量を抽出する抽出工程と、識別子と対になった暗号鍵を用いて、前記特徴量を暗号化することにより暗号化データを生成するデータ生成工程と、これらの識別子と暗号化データとをリライタブルメディアに付加しておく付加工程と、認証を確認する確認者の指示により、識別子を基に暗号鍵を取得し、暗号化データを復号した特徴量と表示データの特徴量とが一致するか否かを判定する判定工程とからなる改竄防止署名方法を実現するものであり、この発明によれば、表示データとともに認証時の特徴量が付加されるので、リライタブルメディア単体で、表示データに認証後の改竄があるか否かを簡単に判別することができる。

【0085】

本発明の改竄防止署名プログラムを記録したコンピュータ読み取り可能な記録媒体は、書き込みおよび消去可能な状態で記憶されている表示データを表示するリライタブルメディアに表示された表示データを認証するリライタブルメディアの改竄防止署名方法を実現するための改竄防止署名プログラムであって、表示データを認証した認証者の指示により、表示データを読み込んで生成した画像データから特徴量を抽出する抽出工程と、識別子と対になった暗号鍵を用いて、前記特徴量を暗号化することにより暗号化データを生成するデータ生成工程と、これらの識別子と暗号化データとをリライタブルメディアに付加しておく付加工程と、認証を確認する確認者の指示により、識別子を基に暗号鍵を取得し、暗号化データを復号した特徴量と表示データの特徴量とが一致するか否かを判定する判定工程とからなる改竄防止署名方法を実現する改竄防止署名プログラムを記録した

ものであり、表示データとともに認証時の特徴量が付加されるので、リライタブルメディア単体で、表示データに認証後の改竄があるか否かを簡単に判別することができる。

【図面の簡単な説明】

【図 1】

本発明の改竄防止署名システムの実施の形態 1 を示す説明図である。

【図 2】

図 1 に示す改竄防止署名システムとともに使用されるリライタブルメディアの一例を示す説明図である。

【図 3】

本発明の改竄防止署名装置の一実施の形態を示す説明図である。

【図 4】

本発明のリライタブルメディアの改竄防止署名方法の一実施の形態のうち署名を書き込む手順を示すフローチャートである。

【図 5】

本発明のリライタブルメディアの改竄防止署名方法の一実施の形態のうち署名を確認する手順を示すフローチャートである。

【図 6】

本発明のリライタブルメディアの改竄防止署名方法の一実施の形態のうち特徴量を抽出する手順を示すフローチャートである。

【図 7】

図 6 に示す特徴量を抽出する手順を実施した際に得られる画像データの一例を示す説明図である。

【図 8】

リライタブルメディアの水平線と読み取りにおける水平線との角度差がある場合の説明図である。

【符号の説明】

10 a, 10 b 改竄防止署名装置

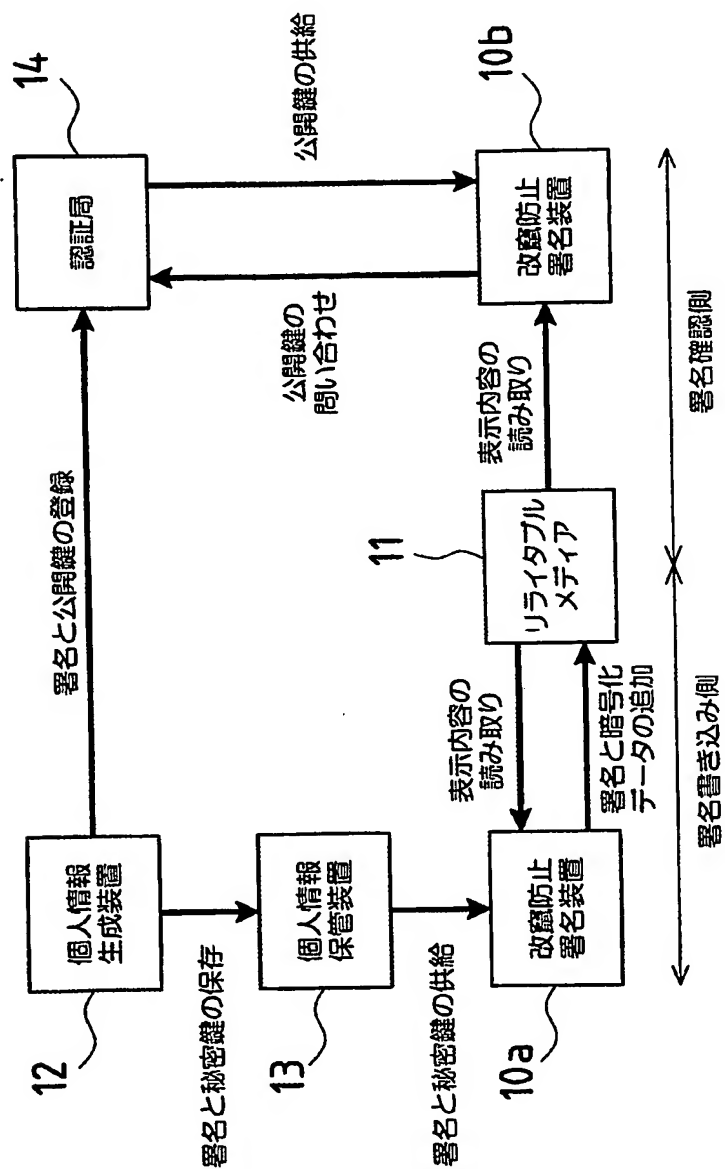
11 リライタブルメディア

- 12 個人情報生成装置
- 13 個人情報保管装置
- 14 認証局
- 30 メディア読み取り部
- 31 領域認識部
- 32 入力補正部
- 33 特徴抽出部
- 34 メディア書き込み部
- 35 暗号化・復号化部
- 36 コンソール
- 37 コントローラ
- 38 認証局通信装置
- 39 個人情報保管装置 I / F
- 50 スキュー角度
- 51 周辺エッジ角度

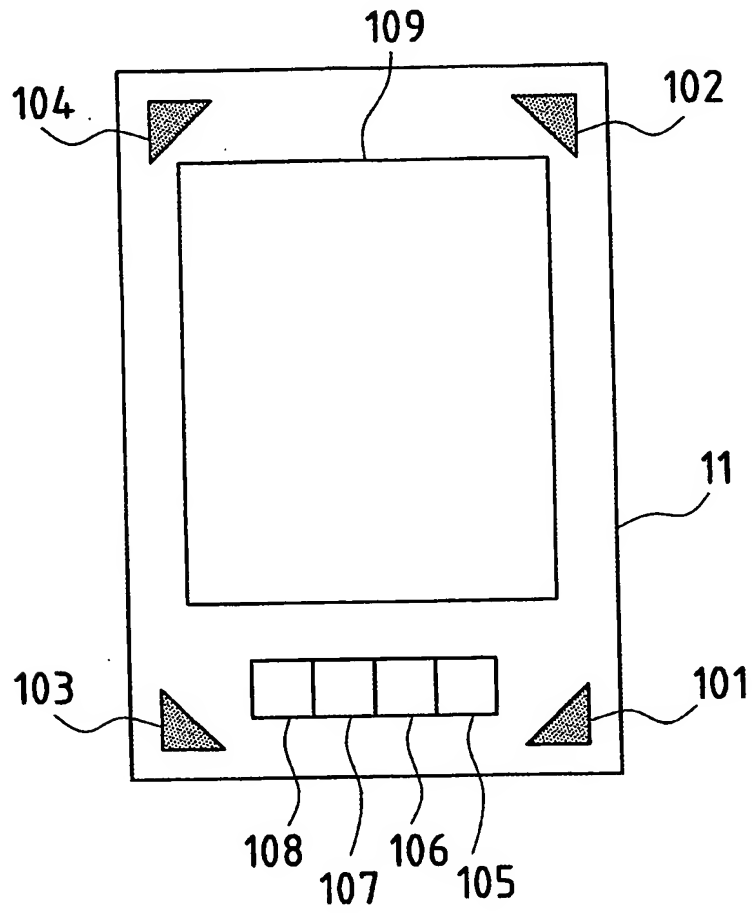
【書類名】

図面

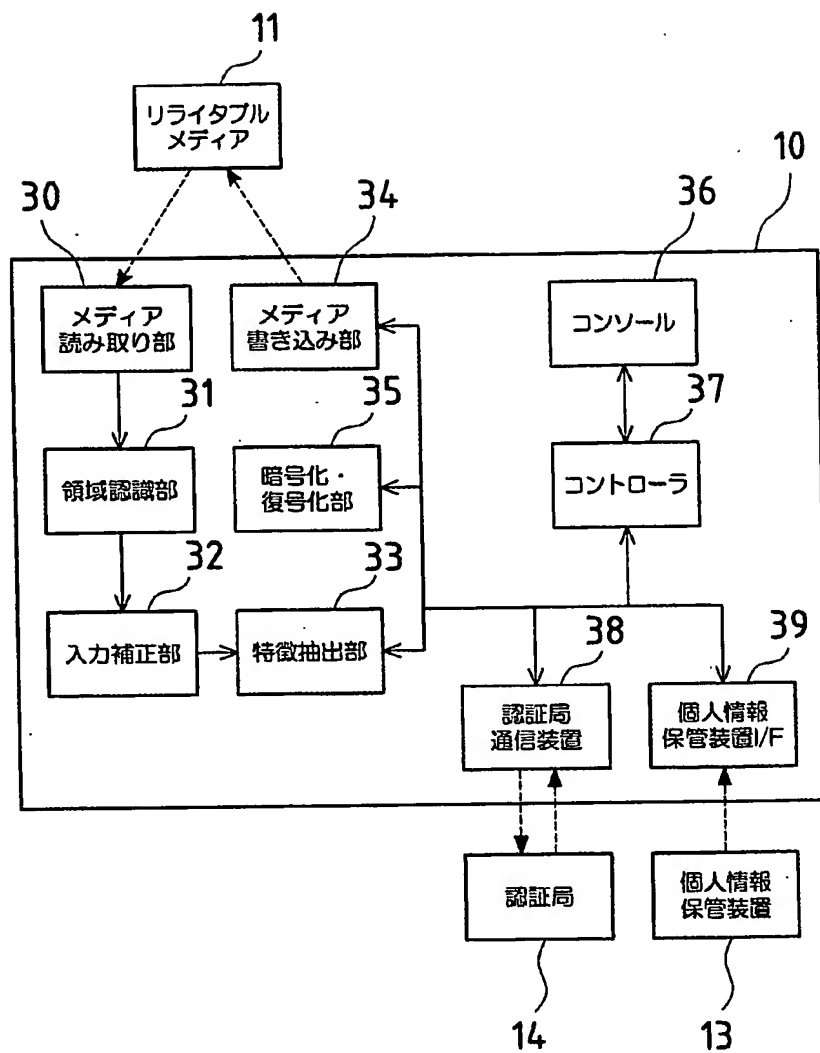
【図 1】



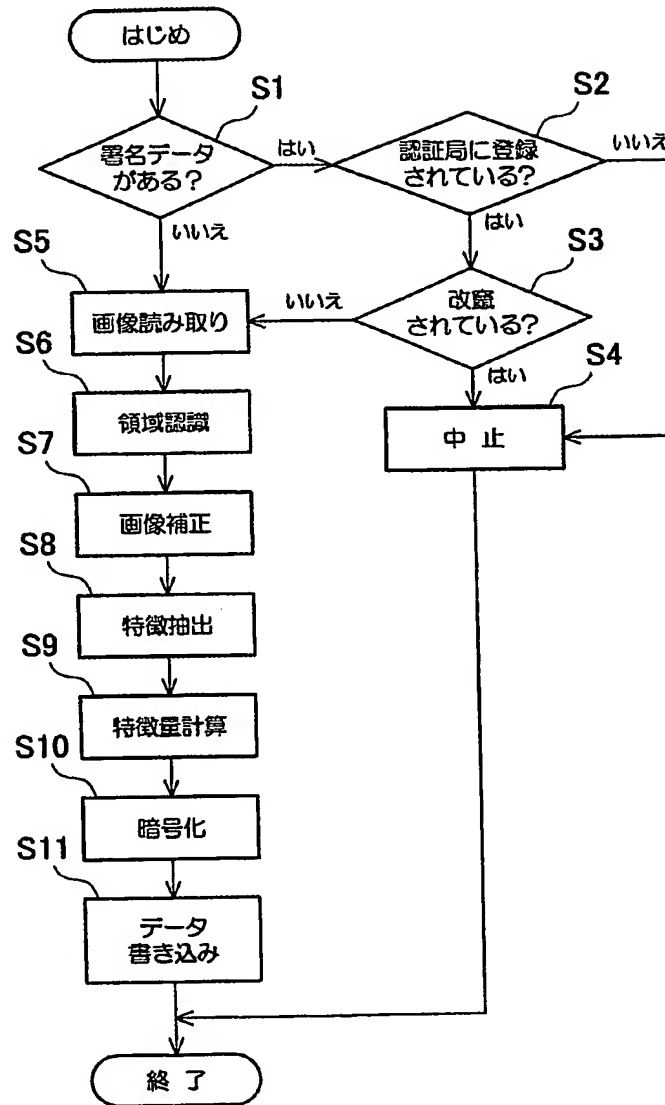
【図2】



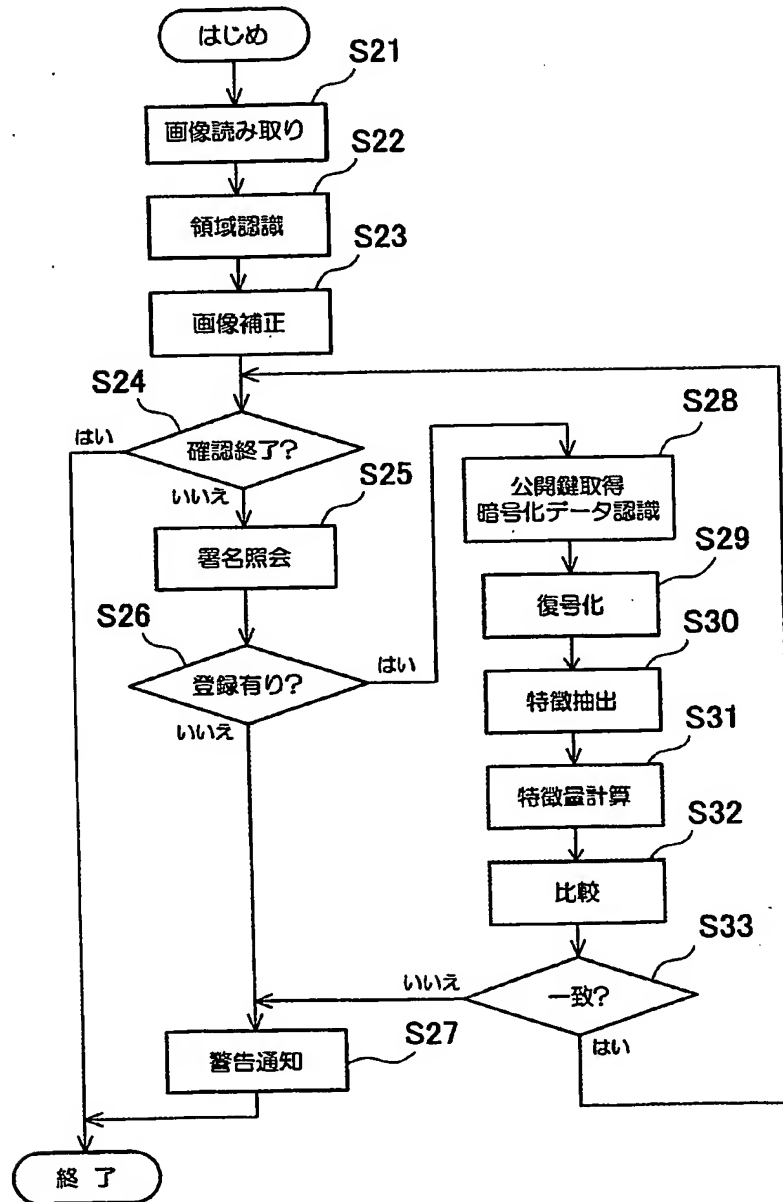
【図3】



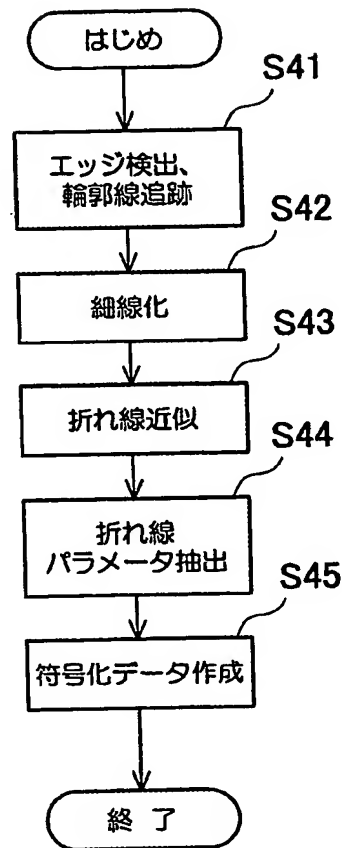
【図 4】



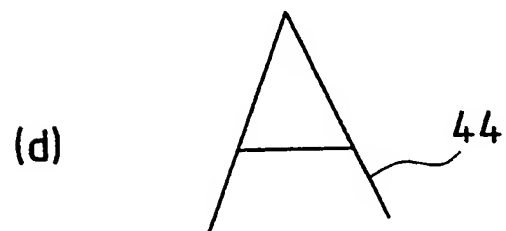
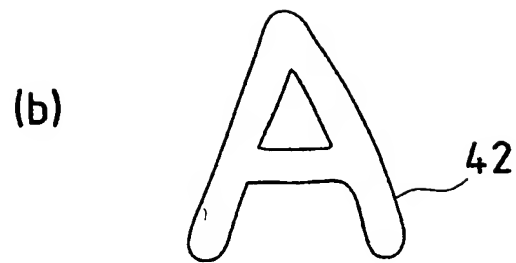
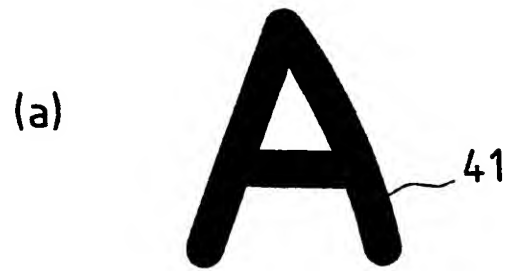
【図 5】



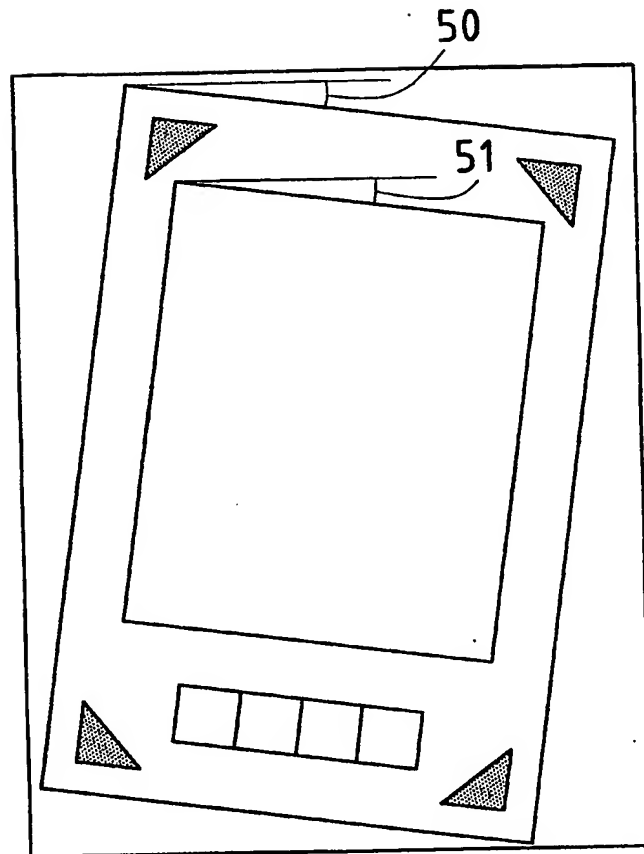
【図 6】



【図7】



【図 8】



【書類名】 要約書

【要約】

【課題】 リライタブルメディア単体で、表示データに認証後の改竄があるか否かを簡単に判別することを可能とする

【解決手段】 表示データを認証した認証者の指示により、画像データの特徴を表す特徴量を抽出する特徴抽出部 33 と、識別子と対になった暗号鍵を用いて特徴量を暗号化することにより暗号化データを生成し、かつ、暗号化データを特徴量に復号化する暗号化・復号化部 35 と、識別子と暗号化データとをリライタブルメディアに付加するメディア書き込み部 34 と、復号化された特徴量と表示データを読み込んで生成した画像データから抽出した特徴量との一致を判定するコントローラ 37 とを備えている。

【選択図】 図 1

特願 2002-201444

出願人履歴情報

識別番号

[000005049]

1. 変更年月日

1990年 8月29日

[変更理由]

新規登録

住所

大阪府大阪市阿倍野区長池町22番22号

氏名

シャープ株式会社